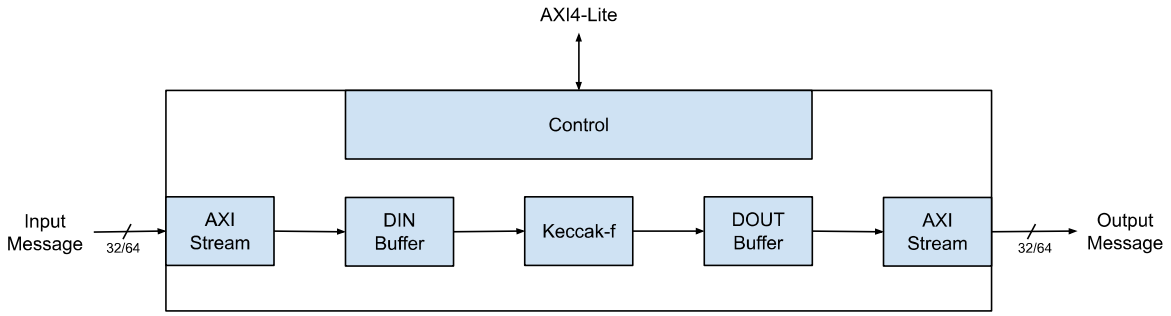
KiviCore
Secure Solutions

SHA-3 Crypto Engine

Introduction

The SHA-3 - secure hash algorithms - crypto engine is a hardware accelerator for cryptographic hashing functions. It is an area efficient and high throughput design and compliant to NIST's FIPS 202 standard. Additionally it supports all SHA-3 hash functions - SHA-3-224, SHA-3-256, SHA-3-384 and SHA-3-512 - as well as extendable output functions (XOF) - SHAKE-128 and SHAKE-256. It provides full protection against time-based side channel attacks (SCA). Automatic bit and byte padding is included.
The SHA-3 crypto engine is an IP core and built with a focus on simplicity and seamless integration, while also following coding and verification practices in the industry. It operates in a single clock domain and has been extensively verified.
The SHA-3 IP core offers a versatile solution for maintaining data integrity and verifying authentication across various applications. Its applications span a wide range, including Message Authentication Codes (MAC), IPsec and TLS/SSL protocol engines, secure boot engines, encrypted data storage, e-commerce platforms, financial transaction systems, blockchain, or pseudo random bit generation.

Block diagramm



Key Feature

FIPS 202 standard compliant

- SHA-3-224
- SHA-3-256
- SHA-3-384
- SHA-3-512
- SHAKE-128
- SHAKE-256
- automatic padding

Integration

- Secure architecture
- fully synchronous design
- AMBA® IF
- platform independent for FPGA & ASIC

Deliverables

- System Verilog RTL source code
- testbenches
- integration example
- software example source code
- documentation